

**UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WISCONSIN**

ECOLAB Inc., and NALCO COMPANY LLC
d/b/a Nalco Water, an Ecolab Company and/or
Nalco Water,

Plaintiffs,

v.

JESSICA GRAILER,

Defendant.

Case No.: 3:23-cv-00102-wmc

DECLARATION OF BRUCE W. PIXLEY

I, Bruce W. Pixley, declare under penalty of perjury that the following is true and correct:

I. Background

1. I am the Managing Member of Pixley Forensics Group LLC. My responsibilities include assisting corporate clients and law firms in investigations and disputes involving forensic accounting issues, electronic discovery, theft of intellectual property, and computer forensic investigations. In this capacity, I manage teams of forensic examiners and use a variety of technologies to perform data acquisition and analysis of this information.

2. Starting in 2001, I served as a lead instructor of computer forensics, Internet investigations, and network intrusion courses for the California Department of Justice's Advanced Training Center. Additionally, I have been employed as a Master Instructor at Guidance Software, which developed the EnCase computer forensic software. As an instructor, I have taught for over 2,000 hours on the subjects of computer forensics and high-tech investigations. I have developed course training materials and wrote manuals for computer forensic courses such as Advanced Internet Examinations and Network Intrusion Investigations.

3. I possess three professional certifications for my fields of work. I possess the Certified Information Systems Security Professional (CISSP) certification and the GIAC Certified Forensic Analyst (GCFA) certification, which are both ANSI ISO accredited credentials, and the EnCase Certified Examiner certification.

4. Since 2003, I have been retained as a computer forensic examiner and subject matter expert in both criminal and civil matters. I have been qualified as an expert witness in both state and federal courts and testified about the foundation of computer forensics, Windows and Mac operating systems, chat software, Internet and network operations, e-mail, peer-to-peer file sharing, digital photography, recovery of deleted data, and Trojan viruses.

5. Attached as **Exhibit A** to this declaration is a copy of my current Curriculum Vitae, which sets forth in detail additional aspects of my qualifications and background.

6. I have been retained by Quarles & Brady LLP, counsel for defendant, Jessica Grailer, to do the following: 1) conduct a review of the declaration and exhibits of Laurence Lieb; 2) conduct the forensic preservation, and review of Jessica Grailer's personal email and Apple iCloud data; and 3) supervise the forensic preservation and conduct an analysis of Jessica Grailer's personal iPhone.

II. Summary of Opinions and Findings

7. The declaration and exhibits prepared by Mr. Lieb do not support his conclusion that Jessica Grailer "exfiltrated multiple Ecolab files via the Emtec USB drive."

8. Mr. Lieb incorrectly interpreted digital evidence and time stamps that he was relying upon to form his conclusion

9. The exhibits prepared by Mr. Lieb contain duplicate entries, which he uses to significantly increase the number of "exfiltrated" files mentioned in his declaration.

III. Evidence Collected and Data Reviewed

10. On March 8, 2023, I conducted a forensic collection of Jessica Grailer's personal Gmail messages (jessicagrailer@gmail.com) using Forensic Email Collector, version 3.86.0.21.

11. On March 8, 2023, I conducted a forensic collection of Jessica Grailer's iPhone backups from her personal Apple account (jessicagrailer@gmail.com) using Cellebrite Cloud, version 7.60.1.9.

12. On March 8, 2023, I conducted a forensic collection of Jessica Grailer's iCloud data stored in her personal Apple account (jessicagrailer@gmail.com) using Elcomsoft forensic software, Phone Breaker, version 10.12.

13. On March 11, 2023, I supervised the forensic collection of Jessica Grailer's personal iPhone 12 mini (model D52gAP, serial number F71DWSNS0GR9) using Cellebrite UFED4PC, version 7.60.0.222.

14. On February 27, 2023, I received a redacted copy of Mr. Lieb's declaration dated February 21, 2023 (Case: 3:23-cv-00102-slc Document #: 15 Filed: 02/23/23) and redacted exhibits (A through K):

- a. Case: 3:23-cv-00102-slc Document #: 13-4 Filed: 02/23/23;
- b. Case: 3:23-cv-00102-slc Document #: 13-5 Filed: 02/23/23;
- c. Case: 3:23-cv-00102-slc Document #: 13-6 Filed: 02/23/23;
- d. Case: 3:23-cv-00102-slc Document #: 13-7 Filed: 02/23/23;
- e. Case: 3:23-cv-00102-slc Document #: 13-8 Filed: 02/23/23;
- f. Case: 3:23-cv-00102-slc Document #: 13-9 Filed: 02/23/23;
- g. Case: 3:23-cv-00102-slc Document #: 13-10 Filed: 02/23/23;
- h. Case: 3:23-cv-00102-slc Document #: 13-11 Filed: 02/23/23;

- i. Case: 3:23-cv-00102-slc Document #: 13-12 Filed: 02/23/23;
- j. Case: 3:23-cv-00102-slc Document #: 13-13 Filed: 02/23/23; and,
- k. Case: 3:23-cv-00102-slc Document #: 13-14 Filed: 02/23/23.

15. On March 9, 2023, I received a copy of Jessica Grailer's declaration dated March 8, 2023 (Case: 3:23-cv-00102-wmc Document #: 28 Filed: 03/08/23).

IV. Review of Laurence Lieb's Declaration and Exhibits

16. In Paragraph 19 of Mr. Lieb's declaration ("Lieb Declaration"), he described a specific USB storage device being connected to the Ecolab laptop on 1/8/2023, 9:39:51 PM, along with citing a specific Windows registry subkey in the footnote. In Paragraph 20, he describes an iPhone 6S being connected to the Ecolab laptop at exactly the same time, 1/8/2023, 9:39:51 PM, and cites a specific Windows registry subkey in the footnote. Based on my review, it appears that this date and time is critical to his conclusion regarding the USB drive as throughout the remainder of his declaration he focused on activity that occurred on or about this time.

17. His analysis of this date and time is flawed and an experienced and objective forensic examiner would not use these time stamps. These registry subkeys are not an accurate method to determine the date and time of a USB device being connected. When Windows conducts an update, these subkeys along with other subkeys in the System hive will get updated by the operating system with exactly the same time stamp. This time stamp is completely unrelated to any user activity. Even common sense would have any layperson ask the valid question of "how does someone plug in a USB drive and an iPhone at exactly the same time?" An experienced forensic examiner would look at all relevant Windows registry information related to external devices, Windows logs, and Windows event logs. At that time, the examiner

would build a timeline to show device activity. In this case, Mr. Lieb incorrectly used these irrelevant time stamps.

18. In Paragraphs 24 and 25 of the Lieb Declaration, Mr. Lieb claims that Grailer exfiltrated four photographs from her Ecolab OneDrive account on 1/8/2023 at 9:11:06 PM. However, he failed to mention exactly how these files were “exfiltrated.” He cites a reference to Exhibit D, which lists the file names of four files, the “last accessed” time stamp, and the path where these files were stored on the laptop hard drive.

19. The problem with using the Windows file system time stamp of “last accessed” is that Microsoft intentionally disabled that specific time stamp with the Windows 7 operating system, which was released in 2009. Since 2009, experienced forensic examiners analyzing a Windows 7 or future Windows release, such as Windows 10, stopped using the “last accessed” time stamp as a measure to determine user activity. To be clear, the last accessed time stamp still exists as it is part of the design of the NTFS file system, but it is not updated when a file is copied, opened, or somehow “accessed.”

20. In Paragraph 29 of the Lieb Declaration, Mr. Lieb cites four files and a folder stored on the USB drive as being “accessed,” however, he failed to cite when these items were accessed. For reference, he cited a specific Windows jumplist file in the footnote, but failed to mention any time stamps. For reference, a Windows jumplist file maintains 8 different types of time stamps for each separate file/folder entry and he did not list any of them.

21. In Paragraph 30 of the Lieb Declaration, Mr. Lieb claimed that Grailer exfiltrated 159 files on 1/8/2023 at 8:56:32 PM; however, he failed to mention exactly how these files were exfiltrated. As evidence, he cited in his footnote that this information was located in the file

system USN journal and the information is listed in Exhibit E. For reference, the USN journal is maintained by the operating system.

22. When I reviewed Exhibit E, I noticed that the majority of the entries had a time stamp of exactly 1/8/2023, 7:20:38 PM with two entries having a time stamp of 8:48:02 PM. It appears that the files listed in this this exhibit are duplicative and his total count of 161 files is inaccurate.

23. An experienced forensic examiner knows that the USN journal has nothing to do with demonstrating that files were somehow “exfiltrated,” such as being copied to a USB device. The USN journal also includes the activity associated with the file, which is noticeably absent from the exhibit.

24. In Paragraph 31 of the Lieb Declaration, Mr. Lieb claimed that Grailer exfiltrated one PDF document on 1/8/2023 at 8:56:32 PM; however, he failed to mention exactly how this one file was exfiltrated. As evidence, he cited Exhibit F, which lists the single PDF file, the file system “last accessed” date, and the path of where the file was located on the hard drive. As described earlier, the last accessed time stamp is a disabled time stamp and has nothing to do with the user accessing or exfiltrating this file somewhere.

25. In Paragraph 32 of the Lieb Declaration, Mr. Lieb claimed that Grailer exfiltrated 128 Excel documents on 1/8/2023. Again, he failed to mention exactly how these files were exfiltrated. As evidence, he cited Exhibit G, which lists the files, the file system “last accessed” date, and the path of where the files were located on the hard drive. As described earlier, the last accessed time stamp is a disabled time stamp and has nothing to do with the user accessing or exfiltrating this file somewhere.

26. It should be noted that Exhibit G was a little different than the previous exhibits:

a. On page 8 of the exhibit, there are entries for four files: NALCO Evap 1-4-23 (002).xlsx; NALCO Gateway 5G 1-6-23 (002).xlsx; PO493751 (002).xlsx; and wwtrial calcs.xlsx. What makes these entries different is that the files were located in a hidden folder maintained by the Outlook email program. When someone opens an attachment in an email message, the attached file is copied from the email and stored on the hard drive so it can be opened and displayed. At this point, an experienced forensic examiner would have looked at the Outlook data file to see what email messages were being accessed and if any messages were sent around this time.

b. The last entry of Exhibit G on page 9 was related to the cache of the Microsoft Edge web browser and maintained in a hidden folder.

27. In Paragraph 33 of the Lieb Declaration, Mr. Lieb claimed that Grailer exfiltrated 43 picture files on 1/8/2023. Again, he failed to mention exactly how these files were exfiltrated. As evidence, he cited Exhibit H, which lists the files, the file system “last accessed” date, and the path of where the files were located on the hard drive. As described earlier, the last accessed time stamp is a disabled time stamp and has nothing to do with the user accessing or exfiltrating this file somewhere.

28. In Paragraph 39 of the Lieb Declaration, Mr. Lieb claimed that Grailer exfiltrated 66 email attachments on 1/8/2023. While he described the files as “downloaded,” he failed to mention the location of where these files were downloaded and exactly how these files were exfiltrated. As evidence, he cited Exhibit G, which contains duplicate entries and four of the entries were also listed in Exhibit H. As mentioned earlier, if a user is reviewing email and email attachments, that activity is not the same as “exfiltration.”

29. After reviewing Mr. Lieb's declaration and exhibits, I have found that he incorrectly interpreted data and time stamps that he was relying upon to form his conclusion. As part of his declaration, he attached a copy of a free certificate issued by Magnet Forensics dated 10/20/2022 (Exhibit A). This certificate is associated with someone attending their 32-hour class. Additionally, he attached a certificate for attending a 2-day basic forensic course on 5/7/2020 (Exhibit B). As a computer forensics instructor, I am familiar with both of these courses. Unfortunately, these courses just skim the surface of digital forensics and train the student on how to use the vendor's point-and-click forensic software. They do not provide in-depth instruction on how to interpret the digital evidence. That type of knowledge comes from years of experience and advanced level training courses.

V. Review of Jessica Grailer's Collected Evidence

30. I conducted a search of the forensic collection of Jessica Grailer's personal data, which is listed in Paragraphs 10 through 13 above, for files that Mr. Lieb listed as exfiltrated in his declaration and attached exhibits (Exhibits D, E, F, G, H, and K). I did not find any matching files or references to those file names. Since none of the file names matched, I could not find any indication that these files were recently accessed.

31. I conducted a search of the forensic collection of Jessica Grailer's personal data for files that Mr. Lieb listed in his declaration in Paragraph 17, Table A. I did not find any matching files or references to those file names. Since none of the file names matched, I could not find any indication that these files were recently accessed.

//

//

32. In reviewing the backups stored in Grailer's personal iCloud account, there were no stored backups for any other iPhone other than her personal iPhone 12 mini.

Executed this 15 day of March, 2023.

A handwritten signature in black ink, appearing to read "B. Pixley", written over a horizontal line.

Bruce W. Pixley